Meeting Minutes

U.S. Government Facial Recognition Series
FORUM II: *Exploring Interagency Information Sharing Challenges and Best Practices*
Sponsored by the Federal Bureau of Investigation's (FBI) Biometric Center of Excellence (BCOE), in conjunction with the Department of Homeland Security (DHS)

Date: November 2, 2011
Location: BRTRC, 8280 Willow Oaks Corporate Drive, Fairfax, VA 22031
Attendees: See Appendix

Overview and Objectives of Meeting | Mr. Tony Brown, Facilitator

- Welcomed participants to the meeting. Introduced himself and acknowledged those who were at the first meeting.
- Reviewed items in the packet and reminded attendees that the meeting is unclassified.
- Stated that this is the second forum in a four-part series designed to identify the primary legal and policy challenges to the deployment of facial recognition technology (FRT).
- Noted that Forum 3, which will focus on privacy issues, is scheduled for March 14, 2012, and that the date and topic of Forum 4 is TBD.

Mr. Brown introduced Ms. Jennifer Alkire McNally, FBI BCOE, and Mr. Steven W. Cooper, Executive Director, Law Enforcement Information Sharing Initiative Program Management Office, U.S. Immigration and Customs Enforcement, Department of Homeland Security (DHS)

Welcome and Forum Preview | Ms. Jennifer Alkire McNally

- Welcomed participants to Forum 2 of the U.S. Government Facial Recognition Legal Series.
- Introduced herself as the organizer of the series for the FBI BCOE.
- Stated that Bill Casey, BCOE Program Manager, had another commitment and shared his regrets.
- Extended special thanks to those who participated in the first forum.
- Thanked DHS and Mr. Cooper for agreeing to partner on the second forum.
- Noted that, through this facial recognition (FR) legal and policy series, we are:
  - Discussing common challenges to the effective use of FRT.
  - Examining the current state of laws and policies.
  - Setting the stage for the development of laws and policies that will more effectively guide all aspects of FRT.
  - Sharing ways to use FRT to more effectively to accomplish the respective missions.
- Remarked on the timeliness of this series vis-a-vis daily news stories about the use of face biometrics across a multitude of contexts.
- Noted that media coverage has raised FRT's profile in the public consciousness, which necessitates making FRT policy development a higher priority than before.

- Recommended working as a cohesive Federal community to advance FRT in a responsible, mission-effective way.
- Reviewed highlights of Forum 1, including:
  - Created a greater understanding of FRT capabilities and limitations.
  - Determined and prioritized the primary legal and policy challenges to FRT.
- Identified top two issues:
    - Information sharing.
    - Privacy protection - specifically, examining the current state of law and policy and discussing how they might develop to achieve law enforcement/intelligence objectives while protecting privacy.
- Gave a preview of Forum 2, to include identification of better ways to share facial data.
- Commented that:
  - FRT has shown tremendous potential to offer investigative and intelligence leads that have never before been exploited.
  - Enormous populations of face imagery exist, and we need to take advantage of them by resolving issues that impact the ability to share data.
- Encouraged active participation in today's program, which is intended to be collaborative.
- Thanked participants again and introduced Mr. Cooper.

Co-Host Presentation | Mr. Steven Cooper, Executive Director, Law Enforcement Information Sharing Initiative Program Management Office, U.S. Immigration and Customs Enforcement, DHS

- Law enforcement must keep pace with technology.
- Biometrics forms the foundation of DHS's US-VISIT program because they are reliable, convenient, and difficult to forge.
- Facial recognition technology reduces workload, is accurate, easy-to-collect and has tremendous investigative and law enforcement potential.
- FRT may be used instead of fingerprints in some cases.
- Policy must accompany technology.
- Standards are needed that take into consideration image quality and privacy issues.
- FRT is less intrusive and less costly than fingerprint technology.
- System effectiveness can be compromised in certain environments.
- FRT quality must be high and match data verified.
- Privacy issues, fear of abuse, and assumption of privacy in public places are some issues to be addressed.
- FRT has potential to manage records of persons of interest, reduce duplication, and provide many other benefits.
- Mr. Brown reviewed Forum 1 and previewed Forum 2:
  - Forum 1 included a presentation and demonstration of FRT state-of-the-art.
  - Discussed:
    - Whether FR is different from other biometrics.
    - The intended purpose of FR at time of capture.
    - Whether facial images and metadata are personally identifiable information (PII), and how policy should address this issue.
  - Forum 2 will:
    - Establish the legal framework that governs FRT.
    - Explore interoperability issues and agency-specific policies.

    - Foster discussion of how existing law and policy may apply to various hypothetical situations.
    - Achieve an understanding of the current policy and legal landscape including:
        - Where are gaps?
        - How can the community share?
        - What happens as data gets shared?
        - How does the data owner maintain control of their data once shared?
- Forum 2 is intended to elicit group discussion, not to produce policy, authoritative guidance, formal proceedings, or decisions.

Mr. Brown introduced Professor Laura Donohue.

Emerging Technology and the Law | Professor Laura Donohue, Associate Professor of Law, Georgetown University Law Center

- Professor Donohue discussed the Constitutional and statutory framework that governs FRT. Statutory law covers:
    - PII
    - National Security surveillance
    - Criminal law surveillance
- She noted:
    - Currently, there are no Federal statutes governing video surveillance.
    - As a result, courts have applied wire and electronic communications statutes.
- Courts may apply Constitutional law, including the First, Fourth, and Fifth Amendments, to determine legal permissibility of FRT.
- The Privacy Act of 1974 is the primary relevant Federal statute.
    - Under this legislation, any government agency must make information available to the person to whom the information belongs, but there are multiple exemptions (e.g. CIA, criminal law investigations, certain biometric systems).
    - Act was amended in 1988 to address automated matching.
- E-Government Act requires privacy impact assessment (PIA) for each government information system and allows exemptions for sensitive information. PIAs exist for FRT activities.
- The Office of Management and Budget (OMB) oversees compliance with Privacy and E-Government Acts.
- National security surveillance for foreign intelligence matters is governed by the Foreign Intelligence Surveillance Act (FISA).
- Two important judicial decisions in the late 1960s: Katz v. United States and Burger v. New York.
    - Katz involved a bookmaker placing bets from a phone booth. Police had installed a listening device in the booth. Was the placement of the device Constitutional?
        - Court said Fourth Amendment protects people, not places.
        - Established "reasonable expectation of privacy" test, which includes objective and subjective components. Katz was protected because the court determined that he had a reasonable expectation of privacy in the phone booth. Therefore, police should have gotten a warrant to listen to his call.
        - Relevance to FRT: Does an individual have a reasonable expectation of privacy of his/her facial image in a given situation?

    - In Burger v. New York, court held that surveillance requires a warrant describing in detail what and where will be searched. Warrant in Burger was too general.
- At the time Katz and Burger were decided, courts relied on Federal Communications Act (specifically, Section 505, which did not apply to state courts).
- In response, Congress introduced Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (i.e. Wiretap Act). Renamed Title I in 1986 to include electronic surveillance, oral communication, and wire communication.
- Wire communication is afforded the highest degree of protection under the law. It includes any communication that travels over wire.
- Oral communication receives less protection than wire communication. Oral communication is any human utterance with expectation that the speaker is not recorded. All human voice transfer falls under Wiretap Act.
- If audio, it may fall into oral communications, under Title I/III.
- Electronic communication receives the least legal protection. It includes any sound, data, writing, etc. that affects interstate commerce.
- Title I/III does not specifically address video surveillance, but many courts have applied it to video surveillance.
- Consent is a critical element of the Wiretap Act. If an individual consents, his Fourth Amendment rights are waived. Absent consent, law enforcement must apply to a judge for a warrant and show probable cause. Must set forth facts of alleged crime, location, who is involved, and explain the necessity of the search.
- Must minimize the amount of information collected, and it must be specific to the crime.
- This is a more stringent standard than a normal search warrant. A high ranking official at the Department of Justice (DOJ) can sign the warrant, and it must be executed within 30 days. Application for extension must include same information. Statute gives the aggrieved a chance to challenge the data. Exclusion does not apply to electronic communications.
- Two carve-outs: consent and information collected in normal course of business.
- Second part of Title I/III, Stored Communications Act, addresses voluntary and compelled disclosure of stored wire and electronic communications by a third party. For this, there are less rigorous standards and less serious criminal penalties than for the Wiretap Act. Information collected in the normal course of business is exempt (e.g. Yahoo).
- Strong case can be made that when the government collects video, the Wiretap Act is implicated.
- Active (i.e. ongoing) filming in a public place is not covered under Wiretap or Storage Acts. Silent surveillance is not covered. Ninth Circuit Court said there must be probable cause, have exhausted other means, and say why this particular information is vital at this particular time. Video can only be used for a limited duration and collection must be minimized to that which is necessary.
- Courts have held that if there are no governing statutes, a Constitutional analysis is needed.
- Fourth Amendment says people have the right to be secure in their house, person, and effects against unreasonable search and seizure.
- Is video a search or a seizure?
    - Courts generally consider biometrics gathering a search but permit it without a warrant for identification purposes.
    - Nature and extent of physical intrusion are important.
    - Courts look at available technology and whether the activity is being conducted for national security or for a criminal investigation.

    - Additional questions to consider: Is the video enhanced or natural? Were steps taken to ensure privacy? Is it unnecessarily disruptive or invasive?
- Aerial surveillance uses the naked eye doctrine.
    - Flying an airplane over a backyard is not a search.
    - Flying an airplane over an industrial plant might be a search if using technology to see/hear through walls.
    - Mounting video cameras on poles to capture that which is visible to anyone is not a search.
    - The location of the capture is relevant. The home is afforded heightened protections.
- GPS technology and placement of a sensor were the subject of U.S. v. Knotts, in which a court held that if a vehicle with a GPS tracker is traveling in open space, there is no reasonable expectation of privacy. Additionally, a car is not an "effect" under Fourth Amendment, so it receives lesser protection.
- In Kyllo v. U.S., a court held that thermal technology placed outside a home to gather information from inside the home is search, even if the technology itself doesn't penetrate the home.
- Level of intrusiveness analysis factors are:
    1. Does FRT change an object in kind or in degree?
        - Courts prefer degree over kind.
        - Binoculars to enhance vision is an example of difference in degree and, therefore, not a search.
        - GPS is less clear. In Knotts, Justice Rehnquist said the Fourth Amendment does not apply, suggesting GPS may present a difference in degree. He stated that trespass might be an issue. Judge Posner said there is no difference between a GPS chip and police following a vehicle. He suggests that GPS is a difference in kind because a car is not a tracking device.
    2. Is there wholesale collection?
        - Collecting information on many people (a crowd) to obtain information on one person is wholesale collection. Courts have held that this is overly intrusive. Must minimize collection to only what is needed.
    3. Is surveillance prolonged?
        - Example of prolonged surveillance is continuously running cameras with no specific timeframe.
        - Is prolonged surveillance a search? In U.S. v. Maynard, a court found that collecting the whole of a person's movements over a month constitutes a search because no one person would have access to this amount of information, and a reasonable person would not expect this amount of information to be gathered.
        - Minimize your collection to only what is needed.
        - No specific timeframe defines "prolonged."
        - Maynard is currently pending at the U.S. Supreme Court.
- In U.S. v. King, the Ninth Circuit Court held that electronic surveillance is much more powerful than normal surveillance because it is more intrusive. Video and audio are indiscriminate. Adding FRT aspect makes it moreso. Judge Posner commented electronic surveillance is too intrusive for Western cultures.
- In Terry v. Ohio, a police officer patted down a driver as part of a routine traffic stop. Court held this was a search. Police officers must articulate specific and reasonable facts to

demonstrate probable cause before conducting a search. Asking for identification during a pat-down is reasonable.

- The zone of privacy is undefined.
- Where a subject tries to change his appearance through disguise or otherwise, courts have held that this suggests an effort to keep identity private and, therefore, Fourth Amendment privacy protections increase.
- Mounting a camera to peer over a fence violates Fourth Amendment rights because the presence of the fence suggests that steps were taken to protect privacy.
- Professor Donohue's summary:
    - In a public space, reasonable expectations of privacy are diminished, so the Fourth Amendment does not apply to FR in public spaces.
    - The level of intrusiveness is likely to be gauged under the Fourth Amendment.
    - Wholesale and prolonged surveillance impose high legal standard.
    - If a search takes place, it must be justified with a reasonable rationale.
    - In determining whether there a reasonable expectation of privacy with one's own biometrics, the nature of the information obtained is significant.
    - Surveillance technology may be improperly used to monitor political demonstrations or placed outside mosques. As a result, FRT could have a chilling effect on First Amendment rights.
    - The Fifth Amendment protects against self-incrimination. To identify a particular person as being at a specific location at specific time, which is the information that FRT may provide (particularly video surveillance), is more intrusiveness than simply identifying the individual's face.
    - The Fifth Amendment is concerned with the nature and reliability of information. The Fourteenth Amendment does the same for states.
    - Accuracy of a biometric device is critical because accuracy implicates due process rights.

Mr. Brown introduced the next session, covering Government policy issues that overlay the legal aspects of FRT.

Biometric Information Sharing Policy Overview | Mr. Monte Hawkins, Director, Identity Management and Biometrics Policy, White House and Ms. Janice McGowan, Chief, Information Sharing Policy Office, National Counterterrorism Center

- The Intelligence Reform and Terrorism Prevention Act (IRTPA) provided for the National Counter Terrorism Center (NCTC), Transportation Security Administration (TSA), and US-VISIT. It formally mandated that biometric information be shared.
- Homeland Security Presidential Directive (HSPD) 24 was developed by a working group in 2006:
    - President mandated NCTC have access to all agencies' terrorism information.
    - HSPD-24 is currently the only Government-wide policy on biometrics and provides a directive for the collection, use, sharing, and storage of face, finger, and iris for intelligence applications and to ensure mutually compatible systems.
    - NCTC took responsibility for the national implementation plan and for the biometrics and identity management group.
    - Intent is to increase FRT interoperability to the same level as fingerprints.
    - Technical issues can be worked out. Policy and legal issues are more difficult.

    - By authority, certain information is to be accessed only by certain agencies; therefore, when such data passes to NCTC, only selected portions of the data can be shared.
    - It is difficult to get visa, arrival, and departure information about U.S. persons because of heightened privacy protections for U.S. persons.
    - HSPD-24 forces biometric identification into a process. One effort is biographic identification – matching a name with a face.
    - When there is a biometric but no name associated with it, it is labeled a "biometric unknown person" (BUP.) Easier for fingerprints than for face.
    - FR is currently used only for investigative lead purposes, not for positive identification.
    - Biometrics may be seen as a luxury in today's economic environment due to expense.
- Hard drives and DVDs obtained from raids are difficult to analyze because current policies do not allow retention of U.S. persons' information.
    - Must differentiate between U.S. and non-U.S. persons and then delete all U.S. persons' information within 180 days of collection.
    - Deleting U.S. persons' information prevents us from searching against the information later.
    - Masking and hashing rules for U.S. persons are an issue because people do not understand the technology.
    - There is synchronization among agencies on watch-listing.
- Another area we struggle with is classified biometrics.
    - In watch-listing, biometrics are unclassified/for official use only for screening purposes because FRT enables mass collections.
    - Currently, we do not have the capability to find a face in a database without an accompanying name or other biographic information.
    - Intelligence community is trying to work through these and other issues.
    - FR is more problematic than other biometrics for NCTC because of policy and legal issues differentiating between U.S. and non-U.S. persons, specifically that one cannot determine nationality just by looking at a face. Significant time is spent deleting U.S. persons' data.
    - Data providers must be part of policy development because they "own" the data.
- Facial recognition presents challenges that other biometrics do not. For example, in addition to the facial image itself, the location at which the facial image was taken and the individual who took the photo may be evidence.

- Questions from the audience:
    - **Q: What steps can be taken to develop FRT policy?**
        - A: Federal standards are needed to prescribe methods to mask and hash data.
        - Each agency must be comfortable with how its data is managed.
        - The NCTC wants as many photos as possible, but image quality is important for the photo to be useful. Quality thresholds may be different for state and local vs. FBI databases.
        - The NCTC is working on facial image collection standards, as is the Facial Identification Scientific Working Group (FISWG), sponsored by the FBI BCOE.
    - **Q: Every agency must have its own database. Why doesn't NCTC have a Federal database?**

    - A: NCTC doesn't own the data it stores. Agencies want to control the data they collect.
- **Q: Could NCTC have a System of Records Notice (SORN) to include all standards and processes in one central location?**
    - A: It would be difficult for one document to reflect all agencies' requirements, and because NCTC does not own the data it receives, the contributing entity is the appropriate publisher of the SORN.

Mr. Brown introduced Ms. Devabhakthuni to talk about Interoperability and Data Sharing.

Interoperability and Data Sharing | Bharatha "Bea" Devabhakthuni, Management and Program Analyst, Interoperability Initiatives Unit, FBI Criminal Justice Information Services Division (CJIS)

- Said that perhaps the fingerprint sharing model could be leveraged to help with facial image sharing processes and standards.
- Gave a brief history of fingerprint sharing:
    - Impetus for interoperability initiative between FBI's Integrated Automated Fingerprint Identification System (IAFIS) and DHS's Automated Biometric Identification System (IDENT) was the Railroad Killer case. Cooperation between DOJ and DHS resulted in apprehension, but the overall systems were incompatible.
- FBI's Interoperability Initiatives Unit mission facilitates sharing through interoperability of various Federal agencies' fingerprint databases.
- Discussed the evolution of interoperability among systems. In 2008, shared services made searches against full repositories possible.
- Introduction of DHS 10-Print Program was a very important milestone in interoperability.
- Showed chart of interoperability process, from law enforcement agency submitting fingerprints to State Identification Bureau through searching IAFIS database.
- User agreements enable sharing among DOJ, DHS, Department of Defense (DOD), and Department of State (DOS).
- Presented a chart showing that the DHS IDENT system does not directly link to DOD Automated Biometric Identification System (ABIS), but both are linked to FBI IAFIS and communicate through it.
- Noted that 30,000 fingerprint checks are performed per day in IDENT from jurisdictions in 43 states.
- Some users benefit from searches from all three biometric systems. Examples include: FBI Mobile, FBI CJIS Division Bioterrorism Risk Assessment Group, U.S. Coast Guard, and Immigration and Customs Enforcement (ICE) Biometric Identification Transnational Migration Alert Program.
- Challenges result from varying missions and, therefore, varying policy issues.
- Not all submissions are able to search IDENT, but a request is pending.
- Latent Interoperable Pilot from the Texas Department of Public Safety is being conducted.

Mr. Brown encouraged participants to engage with questions and comments. He then introduced the panel below and asked them to talk about routine and special case data sharing and the policy gaps of each.

Survey of Agency-Specific Authorities to Share | Mr. John Boyd, Director, Defense Biometrics and Forensics, Assistant Secretary of Defense, Research and Engineering, DoD; Mr. Timothy Edgar, Information Sharing Environment and former Deputy for Civil Liberties, Civil Liberties and Privacy Office, ODNI; Mr. Edward Fluhr, Policy Section Chief, US-VISIT Program, DHS; Ms. Paula Wulff, Assistant General Counsel, Science and Technology Law Unit, FBI

Mr. Boyd:

- DOD shares facial data with the National Ground Intelligence Center (NGIC), and a SORN exists. DOD has two major FRT applications sets: military operations and access control, both physical and logical.
- DOD has two relevant policy documents: collection of biometrics from non-U.S. persons and collection of biometrics for access to bases (draft).
- DOD is currently reviewing in what cases facial images must be collected and in what cases facial images should be collected.
- There are different ways to share using a control number.

Ms. Wulff:

- FBI is focusing on several biometrics, including FRT.
- There are no established FBI policies specific to facial data sharing.

Mr. Fluhr:

- DHS IDENT stores fingerprints but not photo because of wide variations in image quality.
- DHS collects facial images at borders and other points of entry. Supports the U.S. Coast Guard at sea and U.S. citizenship services and visa services.
- Intelligence agencies have their own guidelines.
- DHS is seeing increased interest by other Federal agencies in FRT. Although the community needs to work together, this requires significant thought to bridge gaps with integrity and transparency.
- Federal policies should be written broadly and not modality-specific.
- Public acceptance of FR law and policy is a huge factor. Aggressive outreach campaigns are needed to help the public understand what we are collecting and why.

Mr. Edgar:

- Supports the National Security Staff through Information Sharing Environment (ISE).
- Biometric technology continues to advance while policy issues remain unclear.
- Discussed two information sharing authorities: Patriot Act and Intelligence Reform and Terrorism Prevention Act (IRTPA)
    - Patriot Act, while not specific to biometrics, tore down barriers between law enforcement and intelligence.
    - IRTPA established the NCTC and ISE.
        - ISE handles information necessary to uncover terrorist groups and protect the homeland, including the identity of suspected terrorists.
        - ISE uses government concept of information sharing. Sharing information among government agencies for anti-terrorism purposes is covered by ISE.
- Getting information to front line people is important and requires standards for information sharing.

- National Information Sharing Exchange Model (NIEM) may provide a model for facial data exchange.
    - NIEM does not currently address face.
    - FRT could benefit by creating a list of potential fields/data types so everyone uses consistent labeling to enable sharing. For example, the quality of a photo and the way the photo was collected may be fields, and responses would be coded to ensure consistency.
- Facial data sharing is highly controversial because many activities are innocent.
- Without the proper guidelines, facial data sharing could infringe on people's rights.
- Authorities may permit or require information sharing; however, they must conform with requirements of the Privacy Act of 1974.
- The accuracy of FR devices varies widely.
- Must have an agency-specific use to adopt FR.
- Court rulings are inconsistent.
- Must be sensitive that we live in a globalized society where U.S. rules may differ from those in other countries.
- Information sharing works in coordination with information security.

Mr. Boyd:

- DOD ABIS stores some facial images. Federal Information Processing Standards (FIPS) protect PII. The policy pyramid determines who can share. The way you share matters.
- DOD has collection standards but they are not implemented consistently. In response, DOD is writing an implementation guide.
- DOD wants to develop one set of standards with a strong configuration. The downside of changing standards is that the algorithm must also be changed.
- Each time a picture is taken of an original image, detail is lost, creating potential inaccuracy.
- Even within DOD, some devices are not tested, which impacts public acceptance. Moving toward a goal that all devices and procedures are tested.

Ms. Wulff:

- Data owner must consent to data being used in a certain way and to sharing data with third parties.

Mr. Brown fielded questions:

- **Q: When data is collected by one group, obtained from another group, should the agency with whom data is shared do a SORN? Should there be a Federal SORN?**
    - A: The data owner must author the SORN.
    - Perhaps the Government should be a steward of data rather than an owner.
    - The Privacy Act is decades behind current technology.
    - Standards, SORNs and a mechanism for redress are needed.
    - Greater standardization occurs if agency-to-agency agreements exist.
    - When DHS shares data with other agencies, an interagency agreement is written, which includes procedures, standards, and provisions for third-party sharing.
    - FBI CJIS Division houses the largest Federal biometric databases: Law Enforcement National Data Exchange (N-DEx) and National Crime Information Center (NCIC), populated by state contributed information. As the steward, FBI/CJIS has a statutory obligation to keep them current. Before any official action is taken, the originator of

the data submission (i.e., the data owner) is advised. A redress procedure in place to correct inaccurate information.
    - DOD uses Memorandums of Agreement (MOAs) with agencies with which it shares information, which detail how data can be used.

- **Q: Does stewardship suggest that we should do away with originating agency controls?**
    - A: No. Sensitive data must be protected. Purposes of sharing may be specified in an agreement and a compliance mechanism established. This would cover the issues that an originating agency would likely be concerned with, reducing the need for its subsequent involvement.

- **Q: Is any agency segregating the biometric data from PII?**
    - A: This gets into whether a facial image can be anonymous.
    - Government is more restrictive than the private sector with regard to information privacy protections. As companies are forced to comply with privacy rules, the Government may benefit.
    - In early fingerprint history, FBI/CJIS Advisory Policy Board expressed concerns about privacy protection in fingerprint sharing. The FBI and DHS attempted to share fingerprint templates, but because they used different templates, it did not work. They then shared pieces of the template, which was successful. Because there is no common algorithm, you need to look at how and what you are sharing to find a workable solution.
    - The FBI's N-DEx uses a color-coded system in which data is color-coded green, yellow or red. Information colored green is shared with everyone; yellow-coded information cannot be shown on screen, but contributor contact information is provided. When information is colored red, the requestor receives no information, but the contributor receives a notification that information it submitted has been hit upon through a search, and the contributor may contact the researcher with further information.
    - In the International Trusted Traveler program, each country operates its own biometric screening. If one country (e.g. the U.S.) denies entry of someone from a participating country (e.g. Canada), a denial notification is dispatched, but it does not include the reason for denial.

- **Q: To what extent does NIEM apply to FRT**?
    - A: NIEM doesn't address FRT, but its approach could be useful to facial image sharing. Practical obscurity no longer exists because of technology.

- **Q: What major facial datasets or "pipelines of information" exist across Federal agencies?**
    - A: DOD shares with other databases through FBI's IAFIS, a tenprint database. Sharing with DHS IDENT is manual but scheduled to be automated by the end of next summer.
    - Modalities used by DOD are fingerprint, palm print, voice, iris, and face.
    - Because collection is stressful in a military theater environment, lack of quality collection is an issue.
    - DHS accepts data from visa applications, ICE apprehensions, and border checks. ICE Secure Communities also runs against IDENT, but is not currently set up for FRT.

DHS Customs and Border Protection (CBP) compares facial images against DOS images. IDENT is moving toward integration of iris functionality.
    - MITRE Corporation and the National Institute of Standards and Technology (NIST) have standards and best practices for image capture and quality.
    - FISWG is developing face standards.

- **Q: What are some additional facial image sharing initiatives?**
    - A: The FBI Face Services Team is an in-house initiative that searches facial images submitted by FBI field agents against several databases to generate lead information. The Face Services Team is developing appropriate policies to govern facial image collection. In the future, the service may be offered to DOD, DOS, and state departments of motor vehicles (DMVs).
    - Currently, face is not often used by DOD because of the limitations in accuracy and speed of results. In the future, facial data will be of interest to the NGIC and Biometrics Identity Management Agency (BIMA).
    - NGIC also has a team working on facial image collection.
    - DHS is interested in the potential of FRT, but reliability and accuracy of the technology prevents wide implementation.

- **Q: Is there a difference in the way biometric information is shared depending upon the modality?**
    - A: Yes, there is a difference with regard to policy for two reasons:
        - Facial images may be obtained without the person knowing it and, therefore, without consent, so it is intrusive.
        - FRT poses higher risk of misidentification than fingerprints.
- DNA is very intrusive because of its ability to reveal more information than can be revealed through a fingerprint or facial image.
- A vast majority of biometric information sharing at DHS involves a person applying for a job or entering the U.S. There is not much difference in the way information is shared at DHS based solely on modality.
- Current laws cover immigration information, and certain classes of people receive additional protections.

- **Q: Are all biometric modalities considered PII?**
    - A: General response was yes. DNA profiles submitted through CODIS are subject to very strict legal and technical standards and levels of protection because DNA is physically intrusive and uniquely identifies a person.
    - The way in which biometrics are collected and will be used can affect legal protections. Intrusiveness and accuracy influence the level of legal protection.
    - A photo or video can provide information about a person's location and activities, which is intrusive.
    - Biometrics provide value to the DOD mission. Facial image collection may be a lesser privacy issue for DOD because of the purposes for which it is collected.
    - Many data elements are used to characterize facial images. Where and why did they consent? Under what authority was the image collected? Other data elements might be included to ensure accuracy.
    - Multimodal captures can raise the accuracy of identification. Huge strides have been made in biometrics over the last ten years.

- **Q: Is there a different standard for retained images versus those that will not be retained?**
    - A: Yes, retention is relevant to the degree of protections imposed.

- **Q: Who should spearhead the development of FR standards?**
    - A: National Institute of Justice is working with NIST on standards development. The National Science and Technology Council could also push standards development forward.

Mr. Brown introduced Mr. Yoneda, who led a discussion of hypothetical information sharing situations to explore the practical applications of existing law and policy and to identify policy gaps.

Case Studies Examination | Facilitated by Mr. Theodore K. Yoneda, Attorney Advisor, Office of the General Counsel, FBI

Case Study #1 addressed the illegal reentry of a felon into the U.S. The discussion included:

- **Q: Where should this information be shared?**
    - A: Border Patrol to FBI. Border Patrol to U.S. Attorney's Office.

- **Q: What types of legal instruments could be used to share information?**
    - A: Memorandums of Understanding (MOU).

- **Q: Would there be information in the MOU to effectuate this sharing?**
    - A: As a practical matter, MOUs are overly general.

- **Q: What are some information sharing challenges?**
    - A: One challenge to the FBI is that state and local law enforcement agencies want identification of a Federal agent. Also, state and locals want the FBI to indemnify them in case they are sued under the Anti-Deficiency Act.

- **Q: Should there be a difference in the way policy addresses various biometric modalities?**
    - A: Yes. A person may not reasonably expect his face to be captured, so policy must address issues of intrusiveness and consent.

- **Q: Should policy address the type of biometric or the way the biometric is collected?**
    - A: Some argue that each modality is unique and should have policy specific to it. Others argue that policy can be written to address all biometric modalities by focusing on broad issues of collection, use, sharing, etc. – issues common to all biometrics.

- **Q: Why shouldn't the Government capture a facial image if it is publically available?**
    - A: Federal government must abide by the Privacy Act.

Case Study #3 involved the collection of a facial image a condition of access to a facility. For example, a Federal agency takes a photo of all visitors. The discussion included:

- **Q: Can images be searched against a known and suspected terrorist (KST) database?**
  - A: Informed voluntary consent is needed. Internal Security Act of 1950 gives DOD a right to search anyone entering a DOD facility.

- **Q: What if we wanted to run the information against a file that contains warrants?**
  - A: Probably not without informed consent or probable cause.

- **Q: Can images be searched against state DMV databases to determine immigration status?**
  - A: North Carolina has statutes that allow certain law enforcement access to its DMV records, but each state is different. Some have laws permitting searches under certain circumstances, others prohibit it, and still others have no law that speaks to the issue.

Case Study #4 referenced Case Study #3 and asked whether there is a difference if the building is a Federal courthouse or Congressional office building? The discussion included:

- **Q: Does notice provided to individuals who enter the facility that their photograph is being taken establish voluntary consent?**
  - A: Depends on whether it is a secure facility, which has heightened restrictions.

- **Q: What about taking photos of a public demonstration to try to spot a terrorist?**
  - A: There are potential First Amendment concerns. Trenton, New Jersey has a pilot program in which everyone coming into the courthouse is photographed. The photo is retained for two years in a stand-alone database. There may be a First Amendment right to enter a courthouse that this program may violate.

Case Study #5 concerned the Government collecting facial images from a number of sources and storing them in a Government database. The discussion was cut short because of time limitations, but included the need to establish the legality of the collection and storage of facial images.

- Eventually, all the case studies above will go to court. It is important to create policies that are reasonable and palatable to the public.

Summary of Proceedings and Introduction to Forum 3 | Mr. Brown

- Mr. Brown talked about how this discussion might result in tangible outcomes. He noted that there is much to be said for initiating this conversation and networking.
- Some key themes from the day include:
  - The law is largely silent on FRT.
  - Standards to guide and coordinate how facial data is shared are of the utmost importance.
  - Data stewardship vs. ownership is a concept that warrants further examination.
  - Consent, intrusiveness, and third party use are among the issues that should be addressed by policy.

- Important to engage the public and to let them know that civil servants are working together to use FRT in a responsible way that will ensure that individual privacy is protected.

Closing Remarks | Mr. Cooper and Ms. McNally

- FRT must be transparent going forward. It must be accurate, include robust privacy safeguards, and be conducted with appropriate policy guidance.
- Minutes will be published to the U.S. Government Facial Recognition Legal Serieswebsite when available.
- Minutes from the first forum are posted to the website.
- Ms. Devabhakthuni's slides will be posted to the website.
- Please complete the evaluation form found in your packet, which will help to frame upcoming forums.
- Next forum is March 14, 2012 and will be devoted to privacy.

Adjourned at 1600

Appendix: Attendees

Last	First	Agency	Title
Ballard	Traci	Department of Homeland Security	Attorney, FOIA, Information Disclosure Officer
Becker	Mark	Department of Homeland Security	Senior Policy Advisor
Bhatia	Anita	U.S. Department of State	Attorney Advisor
Blackburn	Duane	White House	Assistant Director
Boyd	John Michael	Department of Defense	Director, Defense Biometrics and Forensics
Brown	Tony	BRTRC	Senior Vice President
Buhrow	William C.	Biometrics Identity Management Agency	Organizational Operations Chief
Clark	Lloyd	U.S. Marshals Service	Senior Inspector
Consaul	Sheila	BRTRC	Contractor
Cook	Justin	Federal Bureau of Investigation	Management & Program Analyst
Cooper	Steven	Executive Director	Immigration and Customs Enforcement
Cutshall	Charles	Department of Homeland Security	Policy Analyst
Daugherty	Tina	Federal Bureau of Investigation	Training Instructor
Devabhakthuni	Bharatha	Federal Bureau of Investigation	Management and Program Analyst
Dolf	Shelley	Federal Bureau of Investigation	Assistant General Counsel
Donohue	Laura	Georgetown University Law School	Professor
Edgell	Brian	Federal Bureau of Investigation	Unit Chief
Fluhr	Edward	Department of Homeland Security	Chief, Policy Section

Ford	William	Department of Justice	Division Director
Frenkel	Jonathan	Federal Bureau of Investigation	Assistant General Counsel
Frierson	Jane	National Counterterrorism Center	Lead Information Systems Engineer
Givan	Natalie	Federal Bureau of Investigation	Management and Program Analyst
Grant	Chris	U.S. Marshals Service	Program Manager
Gustafson	Paul	U.S. Secret Service	Special Agent
Hawkins	Monte	Identity Management and Biometrics Policy White House, NSS	Director
Horbatak	Michael	BRTRC	Contractor
James	Nicolle	Customs and Border Protection	Program Manager
King	Maurice	Department of Homeland Security	Management and Program Analyst
Lee	Christopher	Department of Homeland Security	Privacy Officer
Linger	Jodie	Federal Bureau of Investigation	Management & Program Analyst
Lowery	Victoria	Department of Homeland Security	Information Security Chief, ISSM US-VISIT
Mazel	Joe	Federal Bureau of Investigation OGC/STLU	Assistant General Counsel
McGowan	Janice	National Counterterrorism Center	Chief, Information Sharing Program Policy Office
McNally	Jennifer	Federal Bureau of Investigation	Management & Program Analyst
Melson	Kenneth	Bureau of Alcohol, Tobacco, Firearms and Explosives	Senior Advisor on Forensic Science, OLP
O'Hearn	Donald	U.S. Marshals Service	Chief , Technical Operations Group
Ongstad	Michael	Defense Privacy and Civil Libertiies Office	Senior Policy Analyst
O'Reilly	Sean		

Pietra	Peter	Transportation Security Administration	Director, Privacy Policy & Compliance
Reimers	Gerald F.	National Ground Intelligence Center	Head Agency Counsel
Schilling	Linda Beth	National Institute of Standards and Technology	Director, Project Management Office
Sherman	Michael	Federal Bureau of Investigation Office of the General Counsel	Assistant General Counsel
Sobel	Ted	Department of Homeland Security	Director, Physical Screening Policy
Sprouse	Doug	Federal Bureau of Investigation	Management and Program Analyst
Stasiuk	Teresa	Office of the Director of National Intelligence	Privacy Advisor
Taylor	Warren	Program Manager	Customs and Border Protection
Trevino	Gabriel		
Williams	Edward	Transportation Security Administration	CJIS Systems Officer
Windbush	Marlon	U.S. Marshals Service	OPSEC Coordinator
Wixon	Henry	National Institute of Standards and Technology	Chief Counsel
Yoneda	Theodore	Federal Bureau of Investigation	Assistant General Counsel
Young	Carla E.	Bureau of Alcohol, Tobacco, Firearms and Explosives	Senior Counsel, Field Operations